IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

DAVID FERSZT, *individually and on behalf of all others similarly situated*, Plaintiff, v. MCLAREN HEALTH CARE CORPORATION, Defendant.	Case No. 4:25-cv-11932 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff David Ferszt ("Plaintiff"), by and through his undersigned counsel, hereby brings this Class Action Complaint on behalf of himself and all other similarly situated persons ("Class Members") against Defendant McLaren Health Care Corporation ("McLaren Health" or "Defendant"), alleging as follows based upon information, belief, and investigation of counsel, except as to the allegations specifically pertaining to himself, which are based upon personal knowledge.

NATURE OF THE ACTION

1. Plaintiff brings this action against Defendant for its failure to properly secure and safeguard individuals' highly valuable personally identifiable information ("PII") and protected health information ("PHI") including, *inter alia*, names, Social Security numbers, health insurance information, dates of birth, and medical information including billing or claims information, diagnosis, physician

information, medical record number, Medicare/Medicaid information, prescription/medication information, diagnostic and treatment information.[1]

2. Health care providers that handle PII and PHI owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that its exposure to unauthorized persons—especially to hackers with nefarious intentions—will result in harm to the individuals to whom the information relates.

3. The harm resulting from a data privacy breach manifests in a number of ways, including identity theft and financial or medical fraud. The exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

4. McLaren Health is a health care system including twelve hospitals and operates Michigan's largest network of cancer centers and providers.[2]

---

[1] *Notice of Data Security Incident*, McLaren, https://www.mclaren.org/main/notice-of-data-security-incident (last visited June 26, 2025).

[2] *About McLaren Health Care*, McLaren, https://www.mclaren.org/main/about-mclaren-health-care (last visited June 26, 2025).

5. In order to provide these services, Defendant is indirectly or directly entrusted with individuals' PII and PHI. As Defendant is or should have been aware, these types of personal and sensitive data are highly targeted by hackers who seek to exploit that data for nefarious purposes. In the wrong hands, these types of sensitive data may be wielded to cause significant harm to Class Members.

6. By collecting and storing individuals' PII and PHI, Defendant has a resulting duty to secure, maintain, protect, and safeguard the PII and PHI with which it was entrusted against unauthorized access and disclosure through reasonable and adequate security measures. Defendant is also well aware that PII and PHI are highly valuable to cybercriminals, making it foreseeable that Defendant would be the target of a cyberattack.

7. Despite Defendant's duty to safeguard the PII and PHI with which it was entrusted, and the foreseeability of a data breach, Plaintiff's and Class Members' sensitive information stored by Defendant on its computer system was accessed and acquired by unauthorized third parties during a data breach that occurred on or between July 17, 2024, and August 3, 2024 (the "Data Breach").[3] The Data Breach resulted in the unauthorized access of the PII and PHI of nearly 743,000 patients.[4]

[3] *Notice of Data Security Incident*, *supra* n. 1.

[4] Bill Toulas, McLaren Health Care says data breach impacts 743,000 patients, BleepingComputer (June 23, 2025), https://www.bleepingcomputer.com/news/security/mclaren-health-care-says-data-breach-impacts-743-000-patients/.

8. As a direct and proximate result of Defendant's failure to implement and follow basic, standard security procedures, Plaintiff's and Class Members' PII and PHI are now in the hands of cybercriminals.

9. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief—risks which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

10. Plaintiff, on behalf of himself and the Class as defined herein, brings claims for negligence, negligence *per se*, unjust enrichment, and declaratory judgment, seeking damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

11. To recover from Defendant from these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendant to: (1) investigate and disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; (2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Defendant;

and (3) provide, at Defendant's own expense, all impacted victims with lifetime identity protection services.

PARTIES

12. Plaintiff David Ferszt is an adult who, at all relevant times, is and was a citizen of the State of Michigan. Plaintiff utilizes McLaren Health' healthcare services.

13. Defendant McLaren Health Care Corporation is a Michigan nonprofit corporation with a principal place of business located at One McLaren Parkway, Grand Blanc, MI 48439.

JURISDICTION AND VENUE

14. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

15. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in the State of Michigan.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) as Defendant resides in this District; a substantial part of the events, acts, and omissions

giving rise to Plaintiff's claims occurred in this District; and Defendant conducts substantial business within this District.

FACTUAL BACKGROUND

A. Defendant Collected and Stored Plaintiff's and Class Members' PII and PHI

17. McLaren Health is a $7.3 billion, fully integrated health care delivery system including commercial and Medicaid HMOs covering more than 732,838 lives in Michigan and Indiana. [5]

18. Upon information and belief, during the regular course of administering their services, Defendant receives, creates, maintains, and handles individuals' PII and PHI. This information includes, *inter alia*, names, Social Security numbers, health insurance information, dates of birth, and medical information including billing or claims information, diagnosis, physician information, medical record number, Medicare/Medicaid information, prescription/medication information, diagnostic and treatment information.

19. Plaintiff and Class Members directly or indirectly entrusted Defendant with their sensitive and confidential PII and PHI and, therefore, reasonably expected that Defendant would safeguard their highly sensitive PII and keep their PHI confidential.

[5] *About McLaren Health Care*, *supra* n. 2.

20. Due to the sensitivity of the PII and PHI that Defendant handles, collects, and stores, it is or should have been aware of its critical responsibility to safeguard this information—and, therefore, how devastating its theft is to individuals whose information has been stolen.

21. By requesting, obtaining, collecting, storing, and deriving a benefit from Plaintiff's and Class Members' PII and PHI, Defendant assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

22. Defendant expressly recognize this duty stating that it "understands that health information about you is private and personal, and we are committed to protecting it. We protect the privacy of your health information because it is the right thing to do. We follow federal and state laws that govern your health information."[6]

23. Despite the existence of these duties, Defendant failed to implement reasonable data security measures to protect Plaintiff's and Class Members' PII and PHI, and ultimately allowed nefarious third-party hackers to access and compromise Plaintiff's and Class Members' PII and PHI.

[6] *Compliance Program and Resources*, McLaren, https://www.mclaren.org/main/notice-of-privacy-practices (last visited June 26, 2025).

B. Defendant is Subject to HIPAA as a Covered Entity

24. The Health Insurance Portability and Accountability Act ("HIPAA") circumscribes security provisions and data privacy responsibilities designed to keep individuals' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of PHI.[7]

25. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI is properly maintained.[8]

26. HIPAA applies to two types of entities: "covered entities," such as a health care provider, a health plan, or healthcare clearinghouse; and "business associates" who are engaged by covered entities to help it carry out its healthcare activities. *See* 45 C.F.R. § 160.103.

[7] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, phone numbers, addresses, any dates relating to an individual (including dates of birth), Social Security numbers, and medical record numbers.

[8] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

27. Upon information and belief, Defendant is a "covered entity" that is subject to HIPAA, because it receives, maintains, and electronically transmits PHI from patients as a healthcare provider.

28. Indeed, whenever Defendant contracts with Covered Entities to provide various business and medical services, HIPAA requires that these contracts mandate that Defendant will use adequate safeguards to prevent unauthorized use or disclosure of PHI, including by implementing the HIPAA Security Rule[9] and immediately reporting any unauthorized use or disclosure of PHI (such as the Data Breach) to affected Covered Entities.

29. Defendant explicitly recognizes this duty by stating, "[w]e are required by law to make sure that health information that identifies you is kept private, to provide you with access to our Notice of Privacy Practices outlining our legal duties concerning your health information…"[10]

30. Despite these assurances and Defendant's duty to safeguard Plaintiff's and Class Members' PHI, Defendant employed inadequate data security measures to protect and secure the highly valuable and confidential information with which

[9] The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. *See* 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[10] *Compliance Program and Resources*, *supra* n. 6.

they were entrusted, resulting in the Data Breach and subsequent compromise of Plaintiff's and Class Members' PHI.

31. By requesting, obtaining, collecting, storing, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PHI from unauthorized disclosure.

32. Further, given the application of HIPAA, and that Plaintiff and Class Members directly or indirectly entrusted their PHI to Defendant in order to use their services, Plaintiff and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

C. The Risks of Storing Valuable PII and PHI Are Well-Known in the Healthcare Industry

33. Given McLaren Health's role in handling sensitive data, Defendant was well aware at all relevant times that the PII and PHI that it obtains, collects, stores, uses, and derives a benefit from is highly sensitive and of significant value to those who seek to use it for wrongful purposes.

34. Defendant also knew that a breach of its computer systems, and the resulting exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI were compromised, as well as intrusion into their highly private health information.

35. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at healthcare partner and provider companies, including NextGen Healthcare, Inc. (1.5 million patients, April 2024); OneTouchPoint, Inc. (4.1 million patients, July 2022), Shields Healthcare Group (2 million patients, March 2022), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020). These breaches put Defendant on notice that its electronic records would be targeted by cybercriminals.

36. PII has considerable value and constitutes an enticing and well-known target for hackers. Hackers can easily sell stolen data, as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[11] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

[11] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

37. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the United States. In 2023, there were 6,670 recorded data breach incidents, exposing over 16.8 billion records. The United States specifically saw a 12% year-over-year increase in data breaches as compared to 2023.[12]

38. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, approximately 2.675 million people reported some form of identity fraud compared to approximately 6.5 million people in 2024.[13]

39. The healthcare industry, specifically, has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[14] Indeed, "[t]he IT environments of healthcare organizations are often complex and

[12] *2025 Global Threat Intelligence Report*, Flashpoint, https://go.flashpoint.io/2025_GTIR (last visited June 26, 2025).
[13] *Insurance Information Institute, Facts & Statistics: Identity Theft and Cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited June 26, 2025); https://www.iii.org/graph-archive/96074 (last visited June 26, 2025).
[14] *The Healthcare Industry is at Risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited June 26, 2025).

difficult to secure. Devices and software continue to be used that have reached end-of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that have been developed to work on specific—and now obsolete—operating systems and cannot be transferred to supported operating systems."[15]

40. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2023, 6,759 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights. Those breaches have resulted in the exposure of 846,962,011 healthcare records, a number that equates to 2.6x the population of the United States.[16]

41. In fact, "[a]n unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services Office for Civil Rights, beating the record of 720 healthcare security breaches set

[15] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA Journal (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records.

[16] Steve Alder, *Healthcare Data Breach Statistics*, HIPAA Journal (May 26, 2025), https://www.hipaajournal.com/healthcare-data-breach-statistics/.

the previous year."[17] In 2023 alone, about one-third of Americans were affected by health-related data breaches.[18]

42. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to medical fraud, identity theft, tax fraud, credit and bank fraud, and more.

43. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

44. The Social Security Administration warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

---

[17] Steve Alder, *Security Breaches in Healthcare in 2023*, The HIPAA Journal (January 31, 2024), https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf.

[18] Ken Alltucker, *Health Care Data Breaches Hit 1 in 3 Americans Last Year: Is Your Data Vulnerable?*, USA Today (Feb. 19, 2024), https://www.usatoday.com/story/news/health/2024/02/18/health-data-breaches-hit-new-record-2023/72507651007/.

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[19]

45. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

46. **Healthcare Records**—As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say,

[19] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[20] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[21]

47. Indeed, medical records "are so valuable because they can be used to commit a multitude of crimes. Healthcare data can be used to impersonate patients to obtain expensive medical services, Medicare and Medicaid benefits, healthcare devices, and prescription medications. Healthcare records also contain the necessary information to allow fraudulent tax returns to be filed to obtain rebates."[22]

48. "In contrast to credit card numbers and other financial information, healthcare data has an incredibly long lifespan and can often be misused for long periods undetected. Credit card companies monitor for fraud and rapidly block cards and accounts if suspicious activity is detected, but misuse of healthcare data is harder to identify and can be misused in many ways before any malicious activity is

---

[20] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[21] *Managing Cyber Risks in an Interconnected World, Key Findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited June 26, 2025).

[22] *Security Breaches in Healthcare in 2023*, *supra* n. 17.

detected. During that time, criminals can run up huge debts – far more than is usually possible with stolen credit card information."[23]

49. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data [to] open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[24]

50. Even if stolen PII and PHI do not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Indeed, even where cybercriminals do not gain access to a complete set of an individual's PII and PHI during a data

---

[23] *Id.*

[24] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

breach, cybercriminals can cross-reference two or more sources of PII and PHI to marry data available elsewhere with criminally stolen data, resulting in complete and accurate dossiers on individuals. These dossiers are known as "Fullz" packages.

51. The development of Fullz packages means stolen PII from a data breach can easily be linked to victims' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information (such as emails, phone numbers, or credit card numbers) is not included in the PII stolen in a specific incident, criminals can easily create a Fullz package that links that information together and sell the package at a higher price.

52. Importantly, once a cybercriminal has a Fullz package, they can use it to commit a host of criminal acts including: credit card fraud, loan fraud, identity fraud, account take overs, medical identity fraud, tax refund fraud, and buy now pay later frauds.[25] Most problematic, however, is that cybercriminals in possession of a Fullz package "are difficult to stop with ordinary online security and ID verification measures because they possess all the information needed to get past typical authentication measures."[26]

[25] Paige Tester, *What Are Fullz? How Hackers and Fraudsters Obtain and Use Fullz*, DATADOME (Mar. 3, 2024), https://datadome.co/guides/account-takeover/what-are-fullz-how-do-fullz-work/.

[26] *Protection Against Fullz and Fraud*, INTEGRITY (Apr. 18, 2022), https://integrity.aristotle.com/2022/04/protection-against-fullz-and-fraud/.

53. Based on the value of individuals' PII and PHI to cybercriminals, and the foreseeability of a data breach, Defendant knew or should have known the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences that would arise if its data security systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. Defendant Breached Its Duty to Protect PII and PHI

54. Around August 5, 2024, Defendant became aware of suspicious activity related to certain McLaren and Karmanos Cancer Institute computer systems. Defendant concluded the investigation on May 5, 2025 and determined that an international ransomware group, INC, gained access to McLaren's network between July 17, 2024, and August 3, 2024.[27]

55. But even if Defendant took steps to ensure the data's deletion, *i.e.*, paid the threat actors a likely ransom to ensure the stolen information's destruction, criminals have no incentive to destroy such valuable information that may be monetized in the future, either through extracting additional ransom payments, or using the data to commit fraud and identity theft. As cybersecurity professional Brian Krebs has noted:

> Companies hit by ransomware often face a dual threat: Even if they avoid paying the ransom and can restore things from scratch, about half

[27] *Notice of Data Security Incident*, *supra* n. 1.

> the time the attackers also threaten to release sensitive stolen data unless the victim pays for a promise to have the data deleted. Leaving aside the notion that victims might have any real expectation the attackers will actually destroy the stolen data, new research suggests a fair number of victims who do pay up may see some or all of the stolen data published anyway.[28]

56. Indeed, McLaren Health cannot reasonably maintain that the stolen information has been destroyed and will not be further disseminated. Defendant's own notice to impacted individuals contains an insert labeled, "Steps You Can Take To Protect Personal Information," which advises them to remain vigilant for incidents of fraud and identity theft, take further actions such as monitoring their own credit records, place a fraud alert or credit freeze on their credit reports.

57. Despite discovering the Data Breach on August 5, 2024, Defendant waited approximately ten months to announce that individuals' PII and PHI had been compromised in the Data Breach.

58. Indeed, Defendant did not begin notifying impacted individuals of the Data Breach until June 20, 2025, when they posted a notice of the Data Breach through a press release.[29]

59. Defendant describes the circumstances surrounding the Data Breach as follows:

---

[28] Brian Krebs, *Why Paying to Delete Stolen Data is Bonkers*, Krebs on Security (Nov. 20, 2020), https://krebsonsecurity.com/2020/11/why-paying-to-delete-stolen-data-is-bonkers/.
[29] *Id.*

> Around Aug. 5, 2024, we became aware of suspicious activity related to certain McLaren and Karmanos Cancer Institute computer systems, the result of our organizations being the target of a cybersecurity attack by an international ransomware group. We immediately launched our emergency response plan and an investigation with the assistance of a third-party forensic specialists to secure our network and to determine the nature and scope of the activity.
>
> Through the investigation, it was determined that there was unauthorized access to McLaren's network between July 17, 2024, and August 3, 2024. As part of our investigation, we undertook a thorough review of the potentially impacted files to determine whether any sensitive information was present. It was through this process, which concluded on May 5, 2025, that we determined which patients' information may have been included in the impacted files.[30]

60. At or around this time—more than ten months after the Data Breach took place—Defendant also began to send notification letters to affected individuals.[31]

61. Defendant indicated that a wide variety of patient PII and PHI was compromised in the Data Breach, including, *inter alia*, names, Social Security numbers, health insurance information, dates of birth, and medical information including billing or claims information, diagnosis, physician information, medical

[30] *Id*.

[31] *2025-06-20 McLaren Health Care Data Breach Notice to Consumers*, Office of the Vermont Attorney General, https://ago.vermont.gov/sites/ago/files/documents/2025-06-20%20McLaren%20Health%20Care%20Data%20Breach%20Notice%20to%20Consumers.pdf (last visited June 26, 2025).

record number, Medicare/Medicaid information, prescription/medication information, diagnostic and treatment information.[32]

62. Upon information and belief, the PII and PHI of nearly 743,000 individuals were affected by the Data Breach.[33]

63. Based on Defendant's own statements, cybercriminals intentionally accessed Defendant's computer systems in an attack designed to access Plaintiff's and Class Members' valuable PII and PHI stored therein, and that these malicious actors were successful in the attack.

64. As a direct and proximate result of Defendant's failure to implement and maintain adequate security measures the PII and PHI of nearly 743,000 individuals—including Plaintiff and Class Members—was accessed and compromised by unknown, malicious actors during the Data Breach. Furthermore, it will be nearly impossible for Plaintiff and the Class to ensure that their stolen PII and PHI have been secured and will not be further disseminated.

E. Defendant Is Obligated Under HIPAA to Safeguard PHI

65. As discussed above, Defendant is a covered entity and is required by HIPAA to safeguard PHI.

[32] *Id.*
[33] Toulas, *supra* n. 4.

66. Defendant is required by HIPAA, 42 U.S.C. § 1320d *et seq*. to safeguard patient health information data and health information transactions.

67. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

68. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media"; "[m]aintained in electronic media"; or "[t]ransmitted or maintained in any other form or medium."

69. Under 45 C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) "identifies the individual"; or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."

70. HIPAA requires Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI they create, receive, maintain, or transmit; (b) identify and protect against reasonably anticipated threats to the security or integrity

of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by their workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et seq*.

71. The Department of Health and Human Services Office for Civil Rights recommends the following data security measures that covered entities, like Defendant, and business associates should implement to protect against some of the more common, and often successful, cyber-attack techniques:

a. Regulated entities should implement security awareness and training for all workforce members and that the training programs should be ongoing, and evolving to be flexible to educate the workforce on new and current cybersecurity treats and how to respond;

b. Regulated entities should implement technologies that examine and verify that received emails do not originate from known malicious sites, scan web links or attachments included in emails for potential threats, and impeded or deny the introduction of malware that may attempt to access PHI;

c. Regulated entities should mitigate known data security vulnerabilities by patching or upgrading vulnerable technology infrastructure, by upgrading or replacing obsolete and/or

unsupported applications and devices, or by implementing safeguards to mitigate known vulnerabilities until an upgrade or replacement can occur;

d. Regulated entities should implement security management processes to prevent, detect, contain, and correct security violations, including conducting risk assessments to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI; and

e. Regulated entities should implement strong cyber security practices by requiring strong passwords rules and multifactor identification.[34]

72. Upon information and belief, Defendant failed to implement one or more of the above recommended data security measures.

73. While HIPAA permits covered entities to disclose PHI to third parties under certain circumstances, HIPAA does not permit covered entities to disclose PHI to cybercriminals, nor did Plaintiff or Class Members consent to the disclosure of their PHI to cybercriminals.

[34] *OCR Quarter 1 2022 Cybersecurity Newsletter*, U.S. Dep't Health & Human Services, (Mar. 17, 2022), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html.

74. As such, Defendant is required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that it acquires, receives, and collects, and Defendant is further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

75. Given the application of HIPAA to Defendant, and that Plaintiff and Class Members directly or indirectly entrusted their PHI to Defendant in order to receive healthcare services, Plaintiff and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep their PHI confidential.

F. Defendant Failed to Comply with FTC Guidelines

76. Defendant is prohibited by the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

77. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices.

According to the FTC, the need for data security should be factored into all business decision-making.[35]

78. In 2016, the FTC updated its publication titled Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.[36] The guidelines recommend that businesses implement the following:

a. Businesses should promptly dispose of personal identifiable information that is no longer needed, and retain sensitive data "only as long as you have a business reason to have it;"

b. Businesses should encrypt sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c. Businesses should thoroughly understand the types of vulnerabilities on their network and how to address those vulnerabilities;

d. Businesses should install intrusion detection systems to promptly expose security breaches when they occur; and

---

[35] *See* Federal Trade Commission, *Start with Security: A Guide for Business* (June 2015), available at: https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

[36] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct. 2016), available at: https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

e. Businesses should install monitoring mechanisms to watch for large troves of data being transmitted from their systems.[37]

79. In another publication, the FTC recommended that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[38]

80. Notably, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the FTC Act. Indeed, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[37] *Id.*

[38] *See Start with Security: A Guide for Business*, Federal Trade Commission (June 2015), available at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

81. Upon information and belief, Defendant failed to properly implement one or more of the basic data security practices recommended by the FTC. Defendant's failure to employ reasonable and appropriate data security measures to protect against unauthorized access to individuals' PII and PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

82. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[39]

83. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[40] Upon information and belief, Defendant failed to adhere to the NIST guidance.

84. Further, cybersecurity experts have identified various best practices that should be implemented by entities in the healthcare sector, including implementing the following measures to defend against common cyberattacks:

---

[39] *See Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards & Technology (Apr. 16, 2018), App'x A, Table 2, available at https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.
[40] *Id.* at Table 2, 26-43.

a. Email protection systems and controls;

b. Endpoint protection systems;

c. Identify all users and audit their access to data, application, systems, and endpoints;

d. Data protection and loss prevention measures;

e. IT asset management;

f. Network management;

g. Vulnerability management;

h. Security operations center & incident response; and

i. Cybersecurity oversight and governance policies, procedures, and processes.[41]

85. Upon information and belief, Defendant's failure to protect massive amounts of PII and PHI is a result of its failure to adopt reasonable safeguards as required by the FTC guidelines, NIST guidance, and industry best practices.

86. Defendant was well aware of its obligations to use reasonable measures to protect individuals' PII and PHI. Defendant also knew it was a target for hackers, as discussed above. Despite understanding the risks and consequences of maintaining inadequate data security, Defendant nevertheless failed to comply with

[41] *HICP's 10 Mitigating Practices*, HHS, https://405d.hhs.gov/best-practices (last visited June 26, 2025).

its data security obligations, leading to the compromise of Plaintiff's and Class Members' PII and PHI.

G. Plaintiff and Class Members Suffered Damages

87. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and members of the Class must immediately devote time, energy, and money to: (1) closely monitor their medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

88. Once PII and PHI are exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly for their entire lives, as a result of Defendant's conduct. Further, the value of Plaintiff's and Class Members' PII and PHI has been greatly diminished by its exposure in the Data Breach.

89. As a result of Defendant's failures, Plaintiff and Class Members are also at a substantially increased risk of identity theft, fraud, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

90. With respect to data breaches specifically in the healthcare sector, a study has found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[42]

91. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[43]

92. The reality is that cybercriminals seek nefarious outcomes from a data breach, and "stolen health data can be used to carry out a variety of crimes."[44]

---

[42] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, Health IT Sec. (Sept. 25, 2019), https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.

[43] *Id*.

[44] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

93. Health information in particular is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[45]

94. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[46]

95. Indeed, many victims of medical identity theft are not aware of the theft until long after it occurs; "[s]omeone may apply for a mortgage, for example, and learn their credit is ruined due to unpaid medical bills for care they didn't receive."[47]

96. Plaintiff and Class Members are at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect the PII and PHI with which it was entrusted.

---

[45] *Id*.

[46] *The Potential Damages & Consequences of Medical Identity Theft & Healthcare Data Breaches*, Experian (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[47] Michelle Andrews, *Someone Could Steal Your Medical Records and Bill You for Their Care*, NPR (July 26, 2023), https://www.npr.org/sections/health-shots/2023/07/26/1189831369/medical-identity-fraud-protect-yourself.

97. Additionally, Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

H. Plaintiff's Experience

98. Upon information and belief, Plaintiff utilizes McLaren Health's healthcare services. Plaintiff provided his PII and PHI, directly or indirectly, to McLaren Health in order to receive medical care. In requesting, obtaining, collecting, storing, using, and deriving a benefit from Plaintiff's PII and PHI, Defendant undertook a duty to act reasonably in their handling of Plaintiff's PII and PHI. Defendant, however, did not take reasonable care of Plaintiff's PII and PHI, leading to their exposure and compromise as a direct and proximate result of Defendant's inadequate security measures.

99. On or around June 20, 2025, Plaintiff received notice from Defendant informing him that his PII and PHI entrusted to McLaren Health was compromised in the Data Breach.

100. As a direct and proximate result of the Data Breach, Plaintiff has suffered actual injury from having his PII and PHI exposed and/or stolen as a result of the Data Breach, including: (a) efforts to mitigate the risk of misuse of his PII and PHI; (b) damages to and diminution of the value of his PII and PHI, a form of

intangible property that loses value when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; and (c) loss of privacy.

101. Further, knowing that hackers accessed and possibly exfiltrated his PII and PHI, and that this information likely has been or will be used in the future for identity theft, fraud, and other nefarious purposes has caused Plaintiff to experience frustration, worry, and stress.

102. As a direct and proximate result of the Data Breach, Plaintiff has been and will continue to be at a substantial and certainly impending risk for fraud and identity theft and its attendant damages for years to come. Such a risk is real and certainly impending, and is not speculative given the highly sensitive nature of the PII and PHI compromised in the Data Breach.

CLASS ALLEGATIONS

103. Plaintiff brings this Class Action on behalf of himself and all other similarly situated individuals pursuant to Rule 23 of the Federal Rules of Civil Procedure.

104. Plaintiff seeks to represent a Class of persons to be defined as follows:

> All individuals in the United States whose PII and/or PHI was compromised in the Data Breach of McLaren Health's systems which occurred between approximately July 17, 2024, and August 3, 2024.

105. Excluded from the Class is Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

106. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when he moves for class certification as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

107. **Numerosity:** The members of the Class are so numerous that the joinder of all members is impractical. Plaintiff is informed and believes, and thereon alleges, that there are at least hundreds of thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 743,000 individuals.

108. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached its duties thereby;

c. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII and PHI;

d. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' PII and PHI;

e. Whether Defendant breached its duty to exercise reasonable care in handling Plaintiff's and Class Members' PII and PHI;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

g. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

h. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

109. **Typicality:** Plaintiff's claims are typical of the claims of Class Members. Plaintiff's and Class Members' claims are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and Class Members each had their PII and PHI exposed and/or accessed by an unauthorized third party.

110. **Adequacy:** Plaintiff is an adequate representative of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the Class Members and has no interests antagonistic to the Class Members. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical, as explained above.

111. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all Class Members is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

112. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical

violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages are common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

113. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that generally apply to the Class making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

114. **Ascertainability:** Class Members are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendant's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

115. Plaintiff restates and realleges the allegations set forth in paragraphs 1 through 114 above as if fully set forth herein.

116. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting PII and PHI relating to Plaintiff and the Class in Defendant's

possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

117. Specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendant's security systems to ensure that Plaintiff's and Class Members' PII and PHI in Defendant's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

118. Defendant's duty to use reasonable care arose from several sources, including but not limited to those identified below.

119. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By receiving, maintaining, and handling PII and PHI that are routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats. Defendant alone controlled its technology, infrastructure, and cybersecurity. It further knew or should have known that if hackers breached its data systems, they would extract sensitive data and inflict injury upon Plaintiff and Class Members. Furthermore, Defendant

knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and Class Members, was the foreseeable consequence of Defendant's unsecure, unreasonable data security measures.

120. Defendant also owed a common law duty because its conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's conduct included its failure to adequately restrict access to its computer networks that held Plaintiff's and Class Members' PII and PHI.

121. Defendant's duty also arose from its position as a covered entity. Defendant holds itself out as a trusted covered entity, thereby assuming a duty to reasonably protect the information it obtains. Indeed, Defendant, which receives, maintains, and handles the PII and PHI with which it was entrusted, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

122. Defendant is subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and Defendant and Class Members. The sources of Defendant's duty are identified above.

123. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, Defendant breached its duties through some combination of the following errors and omissions that allowed the Data Breach to occur: (a) mismanaging its systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards, key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII and PHI.

124. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been accessed and compromised by cybercriminals.

125. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries including:

a. Theft of their PII and PHI;

b. Costs associated with requesting credit freezes;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII and PHI being placed in the hands of criminals;

h. Damages to and diminution in value of their PII and PHI entrusted to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data

against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII and PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members.

126. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

127. Plaintiff restates and realleges the allegations set forth in paragraphs 1 through 114 above as if fully set forth herein.

128. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant or failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendant's duty.

129. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of a data breach involving the PII and PHI it obtained when providing healthcare services.

130. Plaintiff and Class Members are within the class of persons that Section 5 of the FTC Act is intended to protect.

131. Moreover, the harm that has occurred is the type of harm that Section 5 of FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

132. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se.*

133. Furthermore, Defendant is a covered entity under HIPAA, which sets minimum federal standards for privacy and security of PHI. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, Defendant had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class members' electronic PHI.

134. Specifically, HIPAA required Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et. seq*.

135. HIPAA also requires Defendant to provide Plaintiff and Class Members with notice of any breach of their individually identifiable PHI "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach." 45 C.F.R. §§ 164.400-414.

136. Defendant violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI; and by failing to provide Plaintiff and Class Members with notification of the Data Breach without unreasonable delay after its discovery.

137. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect, as they are patients of McLaren Health.

138. Moreover, the harm that has occurred is the type of harm that the HIPAA was intended to guard against.

139. Defendant's violation of HIPAA constitutes negligence *per se*.

140. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered injuries, including those identified above in paragraph 125.

141. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

142. Plaintiff restates and realleges the allegations set forth in paragraphs 1 through 114 above as if fully set forth herein.

143. As a condition of providing its healthcare services, McLaren Health required Plaintiff and Class Members to directly or indirectly entrust it with their PII and PHI.

144. As a result of these transactions, Plaintiff and Class Members entered into implied contracts with McLaren Health by which McLaren Health agreed to safeguard and protect such PII and PHI and keep such PII and PHI secure and confidential from unauthorized access.

145. When entering into these implied contracts, Plaintiff and Class Members reasonably believed and expected that McLaren Health's data security practices complied with its statutory and common law duties to adequately protect Plaintiff's and Class Members' PII and PHI.

146. Indeed, implicit in these exchanges was a promise by McLaren Health to ensure the PII and PHI of Plaintiff and Class Members in its possession would be used to provide the agreed-upon services and that McLaren Health would take adequate measures to protect Plaintiff's and Class Members' PII and PHI.

147. It is clear by these exchanges that the parties intended to enter into implied agreements supported by mutual assent. Plaintiff and Class Members would not have disclosed their PII and PHI to McLaren Health but for the prospect of McLaren Health's promise of services. Conversely, McLaren Health presumably would not have taken Plaintiff's and Class Members' PII and PHI if not for the intent to provide Plaintiff and Class Members with its services.

148. Plaintiff and Class Members would not have provided their PII and PHI to McLaren Health had they known that McLaren Health would not safeguard their PII and PHI as promised or provide timely notice of a data breach.

149. Plaintiff and Class Members fully performed their obligations under their implied contracts with McLaren Health.

150. McLaren Health breached its implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' PII and PHI.

151. As a direct and proximate result of McLaren Health's breach of contract, Plaintiff and Class Members have suffered injuries, including those identified in paragraph 125 above.

152. As a direct and proximate result of McLaren Health's breach of implied contract, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

153. Plaintiff restates and realleges the allegations set forth in paragraphs 1 through 114 above as if fully set forth herein.

154. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

155. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of monies paid for healthcare services or other services. Defendant's business model would not exist save for the need to ensure the security of Plaintiff's and Class Members' PII in order to provide their services.

156. The relationship between Defendant is not attenuated, as Plaintiff and Class Members had a reasonable expectation that the security of their PII and PHI would be maintained when they provided their PII and PHI to Defendant.

157. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Upon information and belief, this financial benefit was, in part, conferred, when Defendant was paid by Plaintiff's and Class Members' PII and PHI to provide its healthcare services. Defendant also benefitted from the receipt of Plaintiff's and Class Members' PII and PHI.

158. Defendant also understood and appreciated that the PII and PHI pertaining to Plaintiff and Class Members was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of the PII and PHI.

159. But for Defendant's willingness to commit to properly and safely collecting and maintaining the security of Plaintiff's and Class Members' PII and PHI, their sensitive information would not have been transferred to and entrusted to Defendant. Further, if Defendant had disclosed that its data security measures were inadequate, Defendant would not have gained the trust of its patients.

160. As a result of Defendant's wrongful conduct, Plaintiff and Class Members suffered damages in an amount equal to the difference between their payments made with reasonable data security and privacy practices and procedures

that Plaintiff and Class Members paid for, and those payments without reasonable data security and privacy practices and procedures that they received.

161. Defendant's enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the collection, maintenance, and inadequate security of Plaintiff's and Class Members' PII and PHI, while at the same time failing to securely maintain that information from unauthorized access and compromise.

162. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

163. Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members. It would be unjust, inequitable, and unconscionable to retain the benefits it received and is still receiving from Plaintiff and Class Members because Defendant failed to adequately implement the data privacy and security

procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal and state laws and industry standards.

164. The benefit conferred upon, received, and enjoyed by Defendant was not conferred gratuitously, and it would be inequitable and unjust for Defendant to retain the benefit.

165. Plaintiff and Class Members are without an adequate remedy at law.

166. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services, or Defendant should be compelled to place a percentage of all future profits into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, designed to represent the value obtained by the use of the inadequately secured PII and/or PHI compromised as a result of the Data Breach.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

167. Plaintiff restates and realleges the allegations set forth in paragraphs 1 through 114 above as if fully set forth herein.

168. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et. seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the

parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Class Action Complaint.

169. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and Class Members continue to suffer injury as a result of the compromise of their PII and PHI and remain at imminent risk that further compromises of their PII and/or PHI will occur in the future.

170. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that, among other things:

a. Defendant owed a legal duty to secure patients' PII and PHI under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendant breached and continue to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

171. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and Class Members' PII and PHI.

172. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of any of Defendant's systems. The risk of another such breach is real, immediate, and substantial. If another breach of any of Defendant's systems occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

173. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

174. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach of Defendant's systems, thus eliminating the additional injuries that

would result to Plaintiff, Class Members, and patients whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for relief as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For compensatory damages on behalf of Plaintiff and the Class;

D. For punitive damages on behalf of Plaintiff and the Class;

E. For an order of restitution and all other forms of equitable monetary relief;

F. Declaratory and injunctive relief as described herein;

G. For disgorgement and/or restitution as the Court deems appropriate, just, and proper;

H. Awarding Plaintiff reasonable attorneys' fees, costs, and expenses;

I. Awarding pre- and post-judgment interest on any amounts awarded;

J. For reimbursement for all costs and expenses incurred in connection with the prosecution of these claims; and

K. Awarding of such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: June 26, 2025

Respectfully submitted,

/s/ Gary F. Lynch
Gary F. Lynch
gary@lcllp.com
Nicholas A. Colella
nickc@lcllp.com
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246

Attorneys for Plaintiff and the Proposed Class